



integratedgroup

# FortiMail

---

Predavač: Ivan Galinac, Integra Group

Gost predavač: Marko Ugrin, Fortinet

Case Study: Tommy d.o.o.

6.10.2021.

# FortiMail

- Rizici email-a
- Što je to FortiMail
- Opcije zaštite i M365 integracija
- Case study
- Novosti u 7.0
- Q&A

# To je samo email. U čemu je problem?

The collage features several news snippets:

- FINRA** (Financial Industry Regulatory Authority) logo and a news release titled "LPL to Pay \$9 Million for Systemic Email Failures and for Making Misstatements to FINRA".
- COMPUTERWORLDUK** (FROM IDG) article: "Surrey County Council hit with £120,000 fine for misdirected emails". The text states: "The Information Commissioner's Office (ICO) has imposed a £120,000 fine on Surrey County Council after the local authority repeatedly sent unencrypted, personal information to the wrong email addresses." Author: Anh Nguyen, June 9, 2011.
- CNBC** article: "Xoom says \$30.8 mln transferred fraudulently to overseas accounts".
- INSIDER** article: "Mattel nearly loses \$3M to a classic phishing scam" by Bryan Clark, 5 months ago.
- INSIDER** article: "CEO fired after 'fake CEO' email scam cost firm \$47m".
- FORTUNE** article: "Fraudsters duped this company into handing over \$40 million" by Robert Hackett, August 10, 2015, 4:25 PM EDT. The article mentions "Ubiquiti Networks disclosed the expensive blunder in a quarterly SEC filing."



verizon<sup>v</sup>

92.4%

of malware are delivered via email

49%

of malware was installed via email attachment<sup>1</sup>



FORTINET<sup>®</sup>

15,071

Unique malware variants in 1Q18, an average of 170 every day of the quarter



\$3.3bn

estimated cost of business email compromise, from 30,787 incidents from June 2016 to May 2018

**Notes/Sources:**

1. Verizon 2019 Data Breach Report. May 2019.
2. Fortinet Threat Intelligence Newsletters, 2018.
3. FBI. IC3. 2017 Internet Crime Report. May 2018.
4. Gartner Market Guide for Secure Email Gateways, June 2019.



Gartner<sup>®</sup>

Security and risk management (SRM) leaders must revisit their organizations' email security architecture in the light of current email threats.

This research note is restricted to the personal use of rdavic@fortinet.com.

This research note is restricted to the personal use of rdavic@fortinet.com.

Technology innovations should be especially to combat email threats through a URL). Organizations should simulate measure, and provide training and course, but neither is such awareness defense against many email threats, should document an email security policy what the intended use of corporate email as easy as possible, and strive for a culture

Differentiating Capabilities

The following capabilities can be used in security products. Due to the lack of proof of concept (POC) in vendor sales

To Protect Against Attachment-Based

Network Sandbox

A network sandbox is used to inspect malicious using other methods. The network (including zip, wsf, js and macros that addition, it should have strong anti-em that attempts to detect that it is being

Content Disarm and Reconstruction

Content disarm and reconstruction (CDR) down files into their discrete components type's original specification, ISO standard near-real-time process is an effective files. Although sandboxing and almost against exploits and weaponized content

To Protect Against URL-Based Advanced

URL Rewriting and Time-of-Click Analysis

Rewrite URLs before they are delivered inspection. This can be used to:

- Disarm the URL (i.e., turn it into a safe URL)
- Replace with text (e.g., "embedded content")

Current Capability

✓ Network Sandbox

✓ URL re-write/  
Time of click analysis

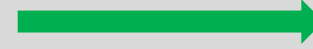
- ✓ DMARC
- ✓ Display Name Spoof Detection
- ✓ Lookalike Domain Detection
- ✓ Anomaly Detection

- ✓ Graymail Handling
- ✓ Data Loss Prevention/Encryption
- ✓ Post-Delivery Clawback
- ✓ SIEM and EDR Integration

For Attachment-based Advanced Threats



For URL-based Advanced Threats



For Imposter-based Advanced Threats



Additional Differentiating Capabilities



Cutting Edge Capability

✓ Content Disarm & Reconstruction

✓ Web Isolation

- 6.x Inbox Profiling/Anomaly Detection
- 6.x Anti-phishing Behavior Training

- ✓ API-based Intra-domain Inspection
- ✓ M-SOAR

...e-of-click analysis protection  
...SEGs, although several have this on their

...secure web gateway (SWG), which is  
...R, SWGs proxy web transactions and  
...a clean rendering of the website content  
...however, active content is executed in a  
...er.

...ing Tactics Used in URL-Based,  
...s

...nd the sender names. Some products  
...ames that the email security  
...uch as senior executives) likely to be  
...sender recipient relationships and seek  
...commonly used keywords in BEC

Conformance on Inbound Email

...writing and conformance (DMARC) on  
...g spoofed external messages from  
...This also checks the alignment of the  
...pe MAIL FROM email addresses.

...as "cousin domains." Most, if not all,  
...ains that should be flagged. Some  
...ams, whereas others require customers

...ient, envelope, content, history and other  
...ats increasingly fly under the radar of  
...ts. Anomaly detection may be able to  
...metry/intelligence enables non-rule-  
...es are sent.

# FortiMail – Secure Email Gateway

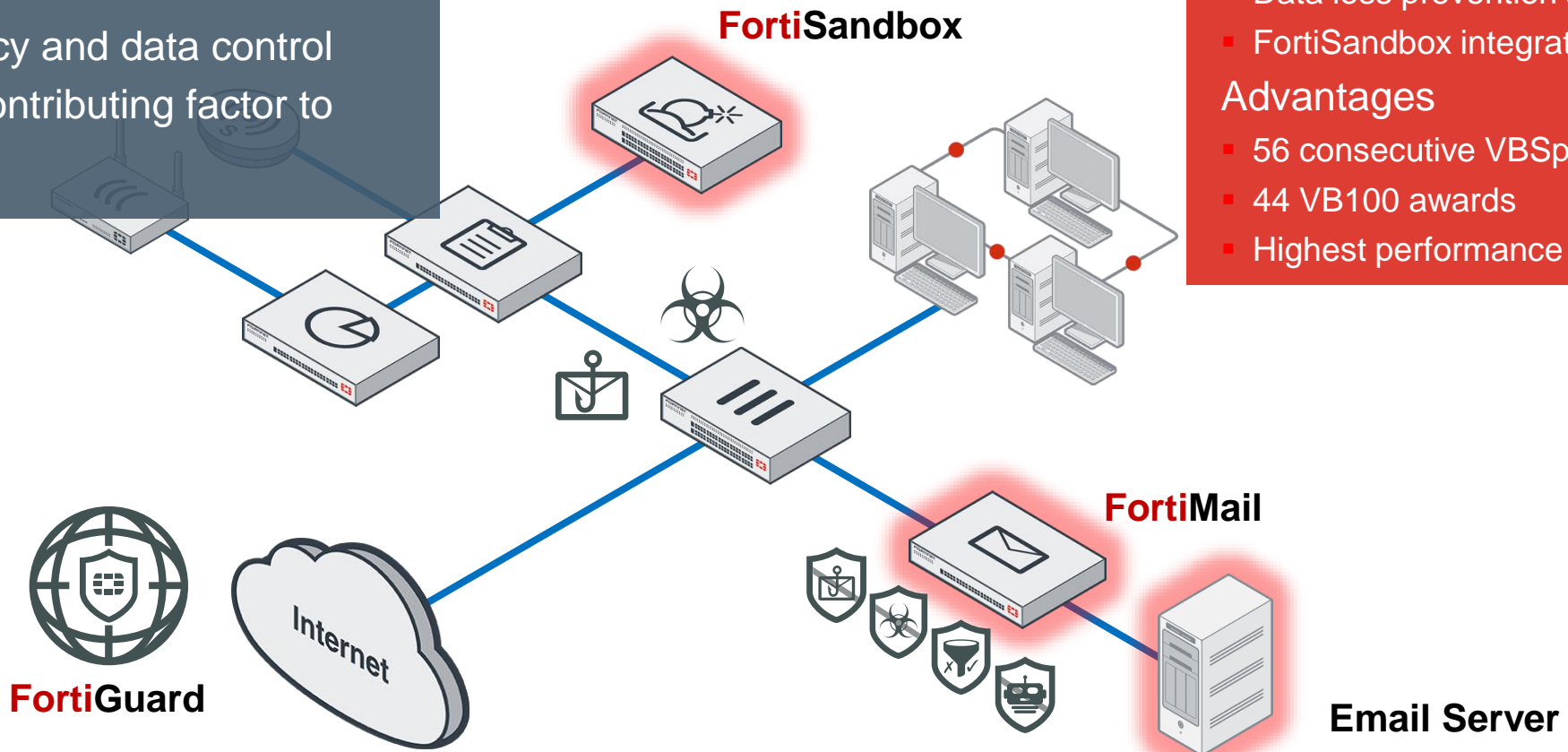
## Primary Challenges

Email common entry point for attackers

- Spam, attachments, phishing
- Targeted attacks

Compliance, privacy and data control

Users are major contributing factor to risk



## Solution

FortiMail Email Security

- Inbound and outbound threat protection
- Data loss prevention and encryption
- FortiSandbox integration

Advantages

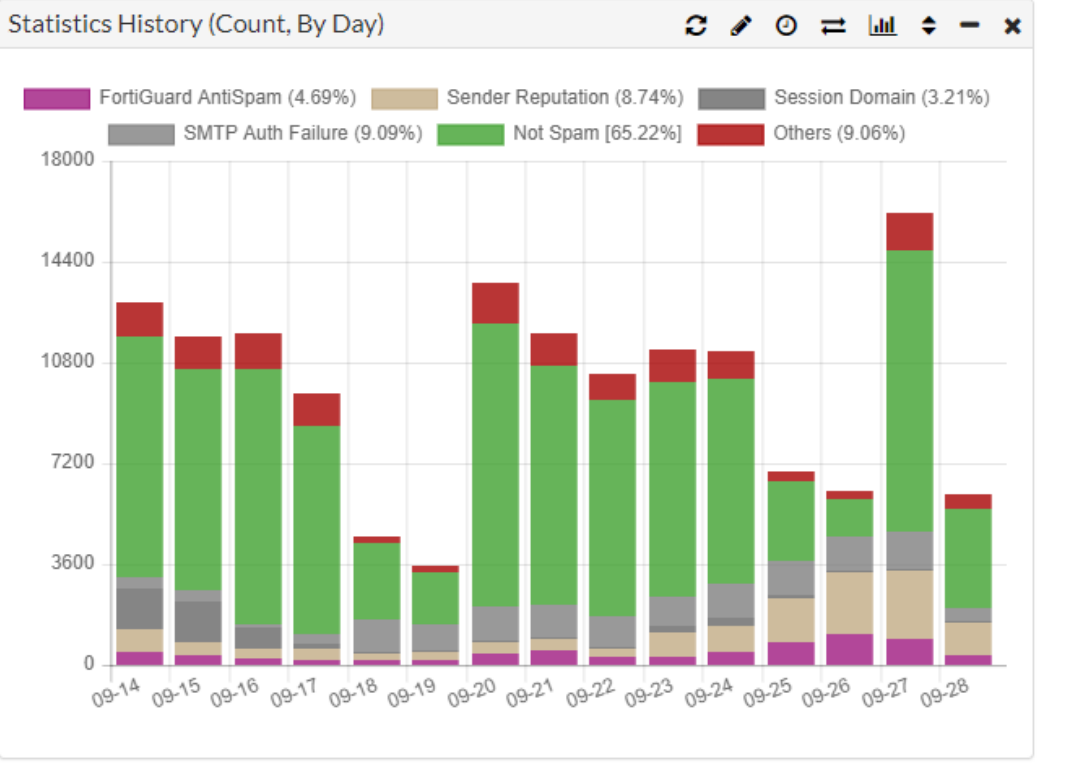
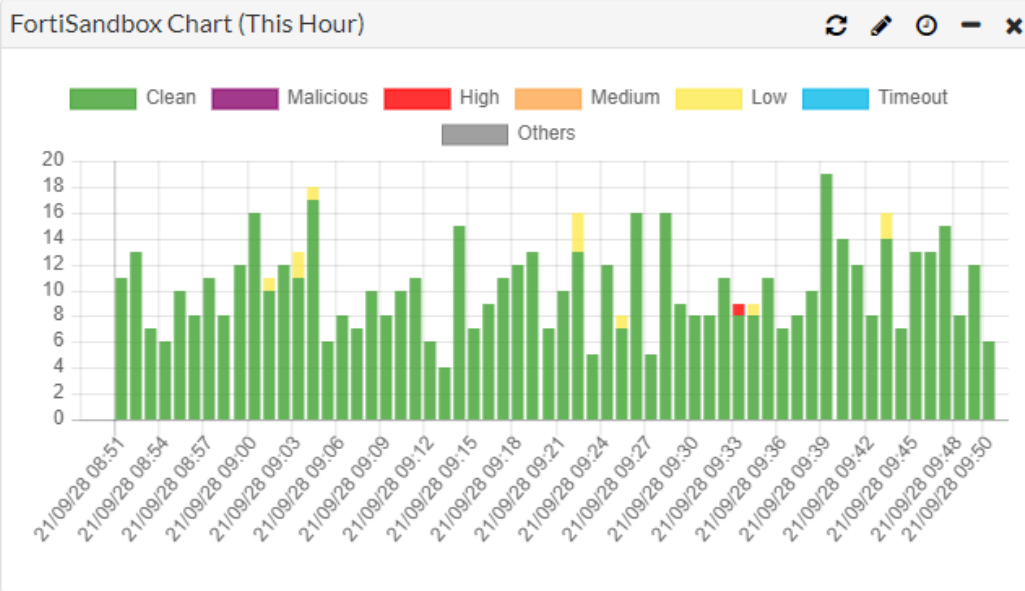
- 56 consecutive VBSpam awards
- 44 VB100 awards
- Highest performance in industry

# FortiMail: Secure Email Gateway

- Dashboard
- FortiView
- Monitor
- System
- Domain & User
- Policy
- Profile
- Security
- Encryption
- Data Loss Prevention
- Email Archiving
- Log & Report

Status Console

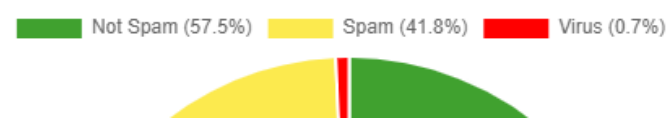
+ Manage Widget    ⌂ Reset Widget



Statistics Summary

Messages	Total	This Year	This Month	This Week	Today	This Hour	This Minute
Access Control-Safe-Relay	6833	6833	1051	59	11	2	0
Bypass Scan On Auth	2237	2237	306	4	1	0	0
FortiGuard AntiSpam-Safe	36	36	0	0	0	0	0
Not Spam	1036311	1036311	165963	14852	3502	827	7
System Safe	167871	167871	93	4	0	0	0

Statistics Summary (Today)





# FortiMail: Secure Email Gateway

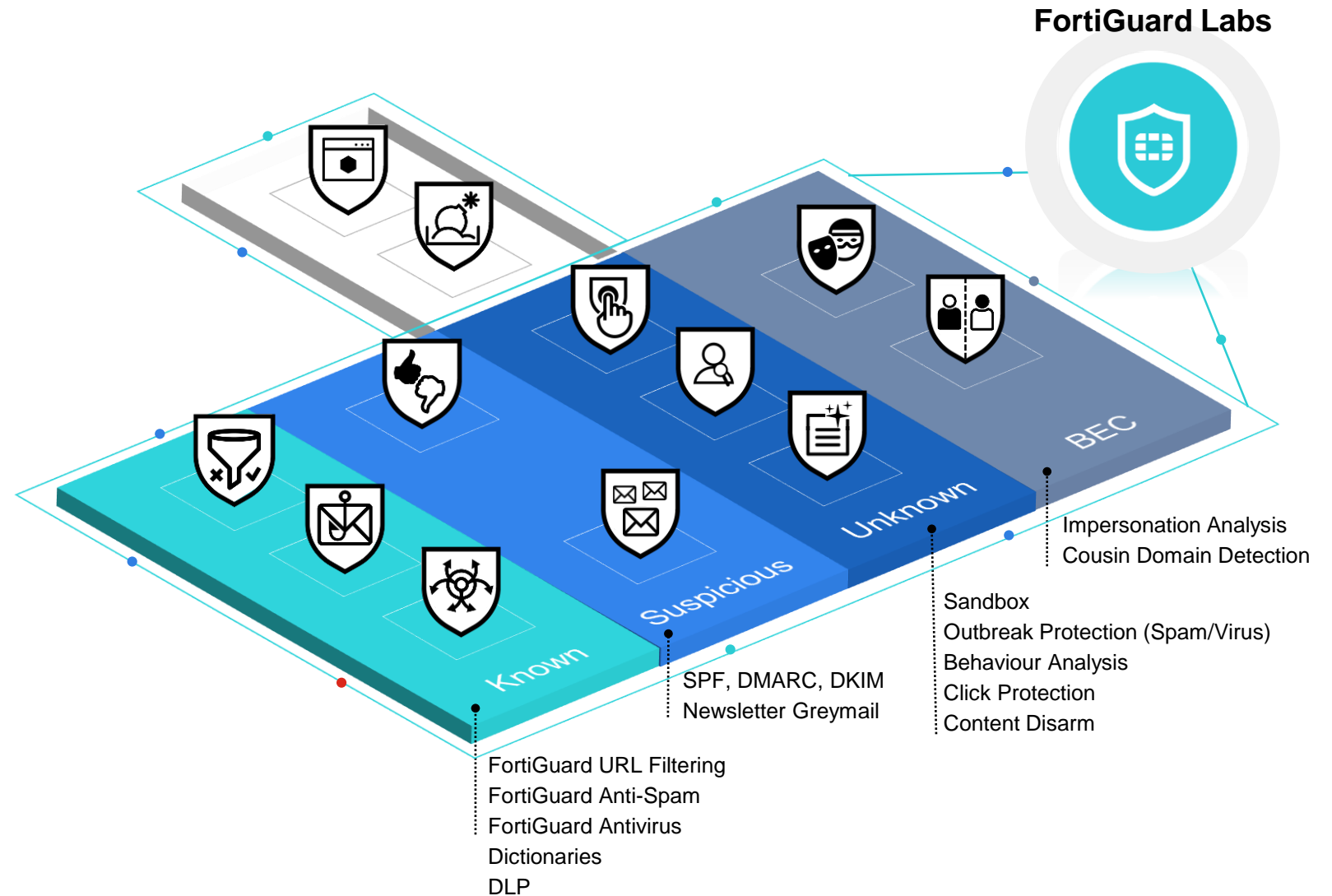
## Advanced multi-layer security against:

- Known threats
- Suspected threats
- Unknown threats/Zero-days
- Impersonation attempts
- Business Email Compromise

## Flexible

- Policies
- Profiles

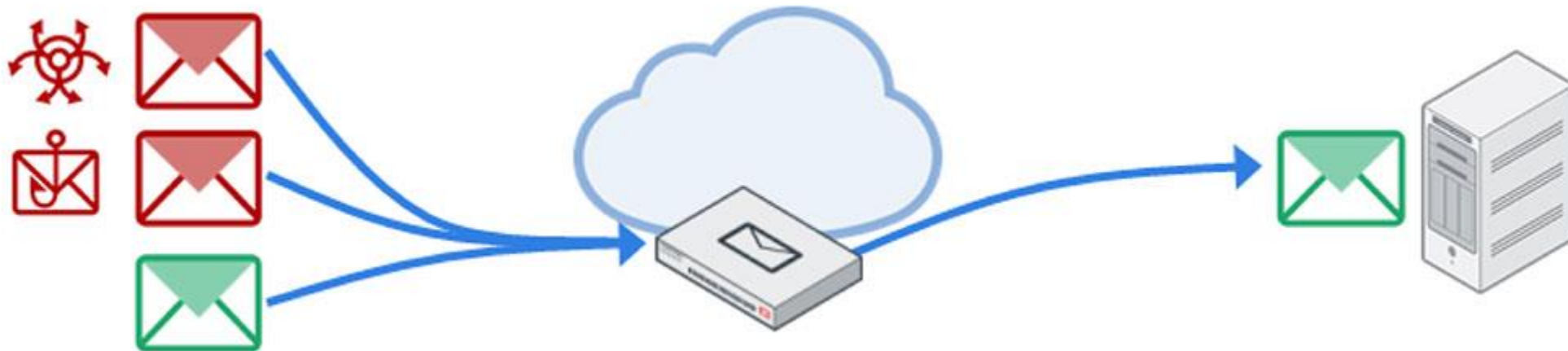
API:  Microsoft 365



## Gateway način rada

### Gateway Mode

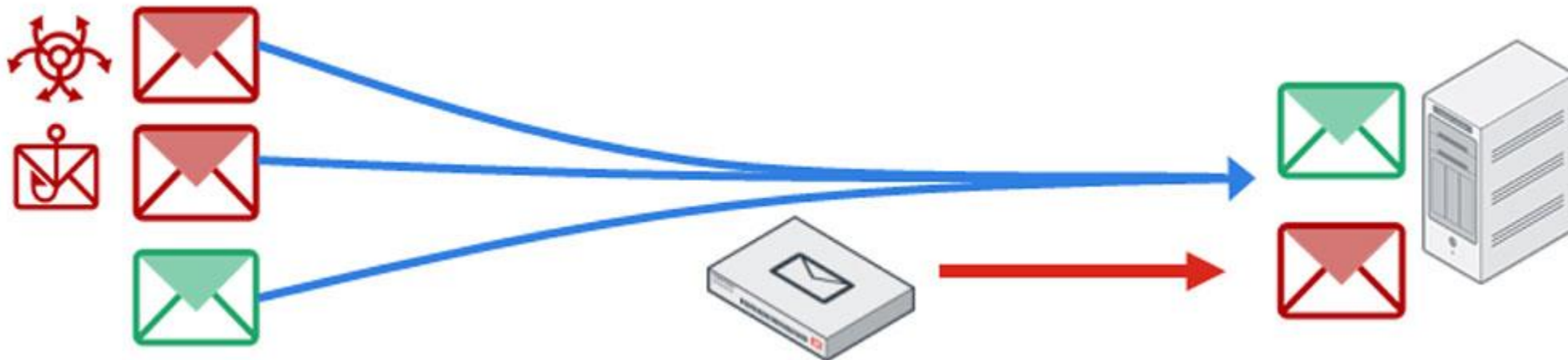
- Inbound and outbound MTA with application-layer security
- Requires a DNS MX record change or a destination NAT rule change
- All inbound email goes through FortiMail first, then is routed to a backend mail server



## M365 API način rada

### Microsoft 365 API Support/Clawback

- Operates out-of-line, scan and clawback threats directly from Microsoft 365 using the Graph API
- Can be used in conjunction with gateway mode



## Transparentni način rada

### Transparent Mode

- DNS MX record, or DNAT rule changes aren't required
- Physically located on the SMTP path
- Intercepts email, even though destination IP address isn't FortiMail



## Serverski način rada

### Server Mode

- Full-featured mail server that has application-layer security
- Receives, inspects, and delivers email to user mailboxes stored in a local database

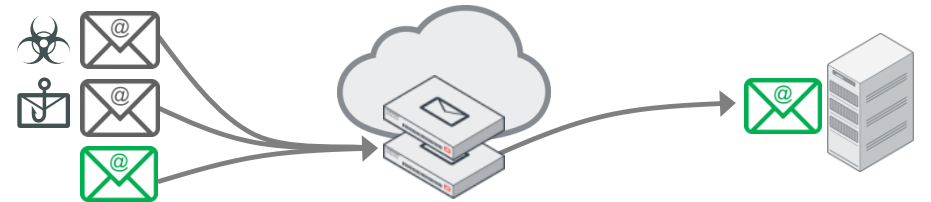


## Deployment opcije

### High Availability and Scalability Options

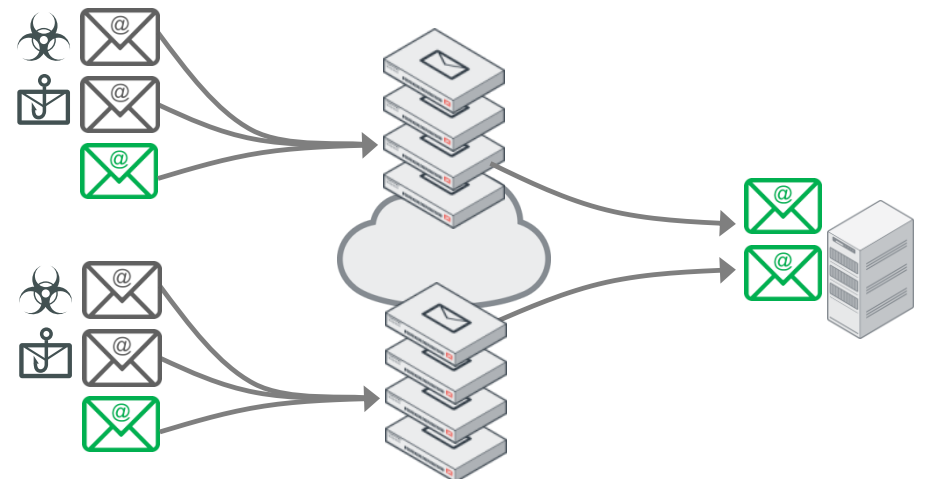
#### Active-Passive Cluster

- **Two-devices, full failover protection**
- Heartbeat and Service Monitoring
- Full mailbox, archive, quarantine, log and queue synchronization



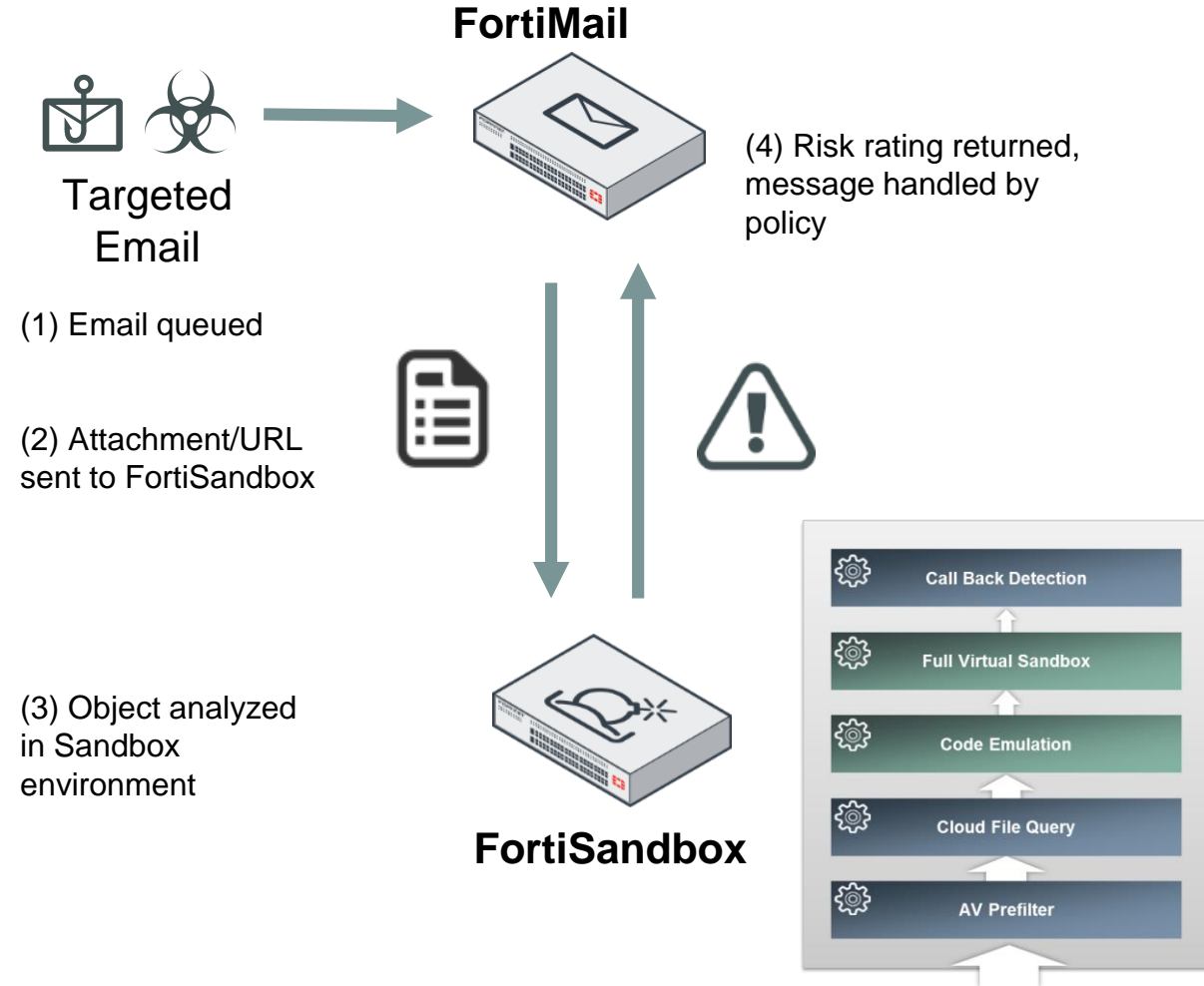
#### Config Only HA

- **Linear scalability suitable for the largest ISPs and Carriers**
- Centralized quarantine, management and IBE
- Enables DR and geographic redundancy
- Load balanced option using FortiADC or third party load balancer



## FortiSandbox analiza prijetnji\*

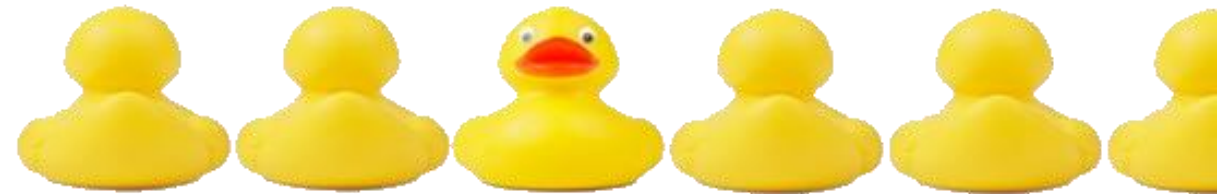
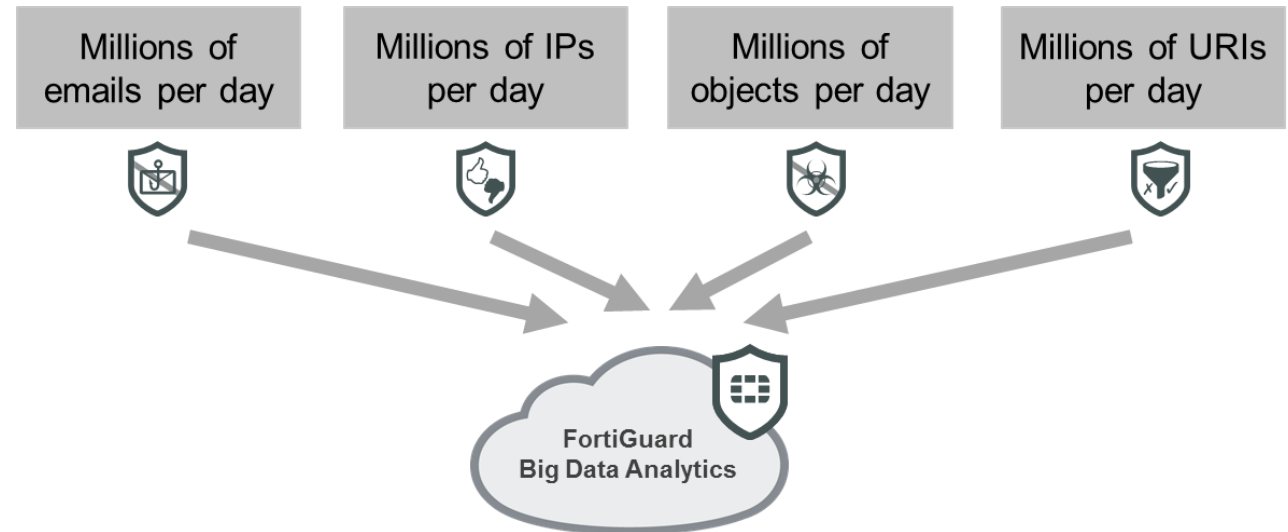
- **On-Premise and Cloud options**
  - FortiSandbox Cloud included in Enterprise ATP Bundle
- **FortiMail queues email and submits files and URLs to FortiSandbox for analysis**
  - AV Pre-filtering
  - Cloud results lookup - is sample already known bad
  - Analyze objects in a virtual sandbox environment
  - Callback detection – does sample try to call home for instructions
  - Assign and return a rating for the submission
  - FortiMail maintains a cache of FortiSandbox results



\* Optional but a core part of an ATP solution

## Obrana od novih prijetnji

- **FortiGuard Virus & Spam Outbreak Protection**
  - Suspicious attachments detected in known spam are blocked until full evaluation by FortiGuard Labs.
  - Cyberthreat Alliance, FortiSandbox Cloud Collaboration, FortiGuard Pre-Signature hashes
- **Behavioural Analysis**
  - Machine learning engine based on previous detections
  - Is behaviour similar to recent signature based detections?





## Prevenција ciljanih napada

- **Content Disarm & Reconstruction**
  - Select URI category to strip when disarming HTML
  - Select a URL filter to selectively disarm URLs in CDR
- **Password Decrypt Office Docs**
  - Password decryption of archives, PDF and Office documents
  - Passwords automatically identified
  - Common password list
  - Admin defined password list
  - Detect passwords in email body

The screenshot shows a Microsoft Word document titled "example.docm - Microsoft Word". The document content includes:

- DOCX test file**
- Purpose: Provide example of this file type
- Document file type: DOCM
- Version: 1.0
- Remark:
- Example content: <https://www.playboy.com>
- Test Data table:

1			
1			
2			
3			
4			

The names "John Doe" for males, "Jane Doe" or "Jane Roe" for females, or "Jonnie Doe" and "Janie Doe" for children, or just "Doe" non-gender-specifically are used as placeholder names for a party whose true identity is unknown or must be withheld in a legal action, case, or discussion. The names are also used to refer to a corpse or hospital patient whose identity is unknown. This practice is widely used in the United States and Canada, but is rarely used in other English-speaking countries including the United Kingdom itself, from where the use of "John Doe" in a legal context originates. The names Joe Bloggs or John Smith are used in the UK instead, as well as in Australia and New Zealand.

Annotations with red arrows point to:

- Remove macros**: Points to the "Developer" tab in the ribbon.
- Neutralize URLs**: Points to the "https://www.playboy.com" link.
- Remove embedded content**: Points to the image placeholder in the text.

**Content Disarm and Reconstruction** dialog box:

- Action: --Default--
- HTML content:  Sanitize HTML content
- Text content:  Convert HTML to text
- MS Office:  Sanitize HTML content
- PDF:  Remove URIs
- Click Protection:

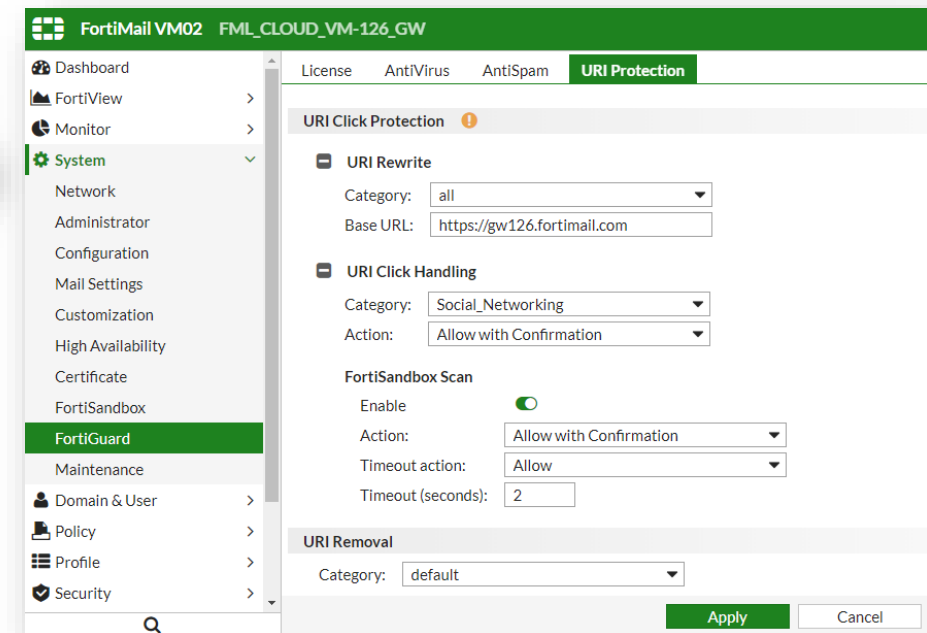
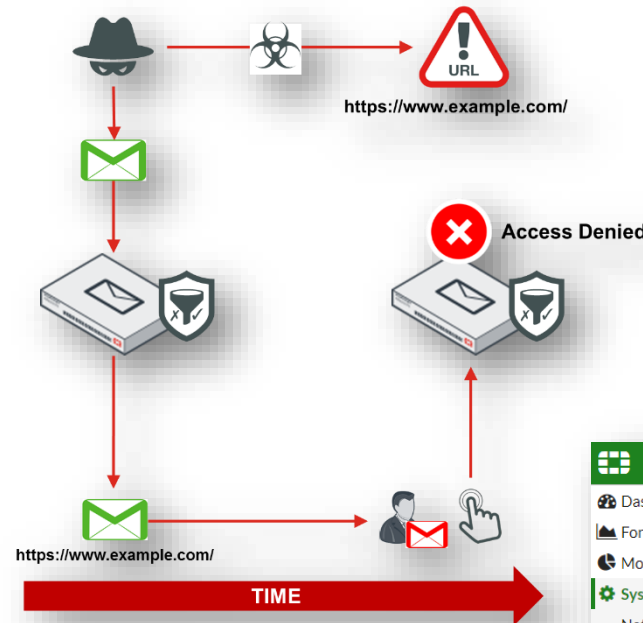
## Prevensija ciljanih napada

- **URI Click Protection**

- Rewrite URLs to point at FortiMail
  - FortiMail rescans when links are clicked to detect status change since first rating
  - New URL Click Protect License

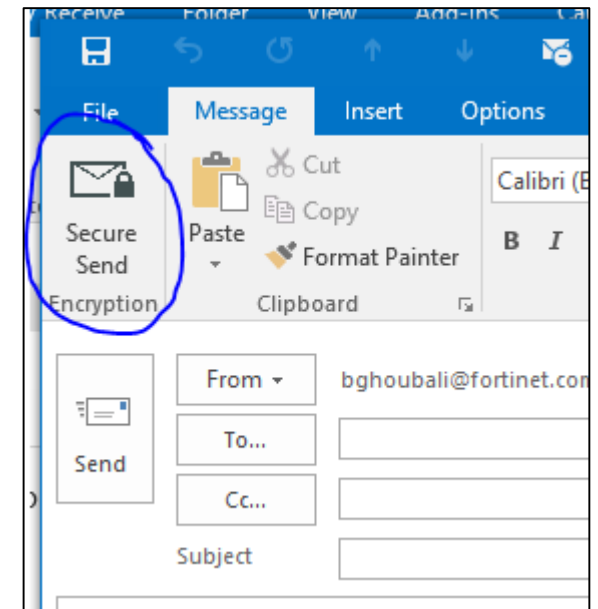
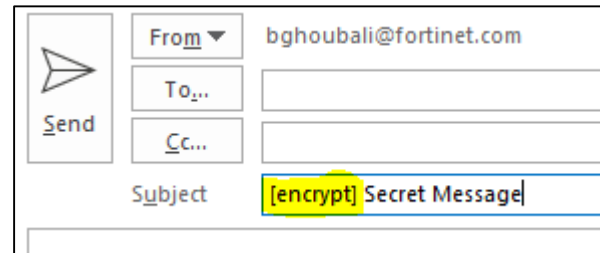
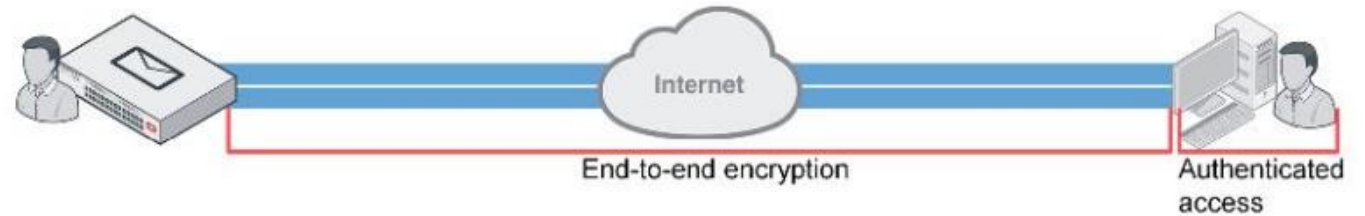
- **Benefit**

- Extends security to the desktop

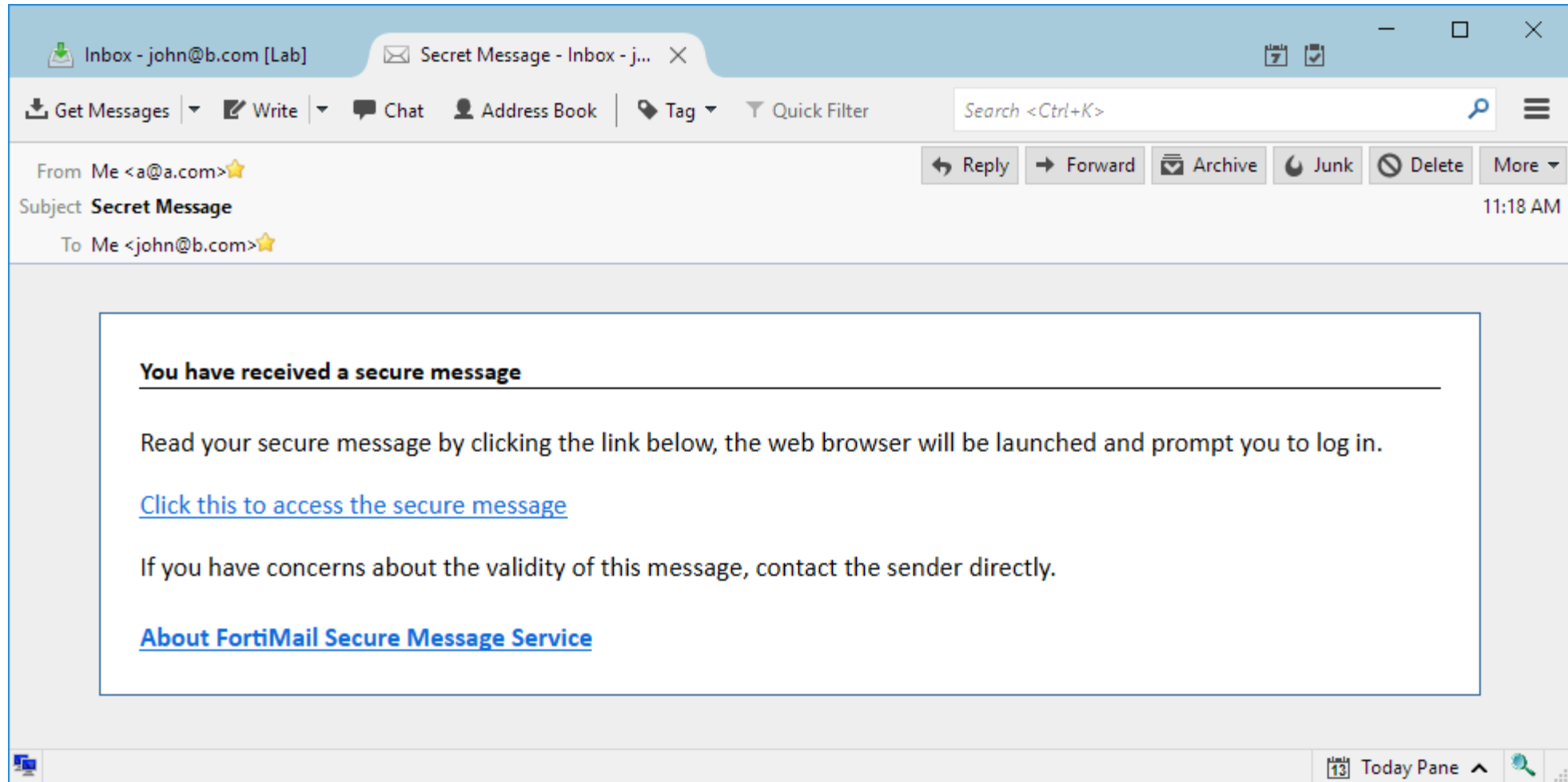


## Identity based encryption (IBE)

- **Identity based encryption**
  - End-to-end enkripcija mail prometa
  - Sigurno slanje osjetljivih podataka, koristi se HTTPS enkripcija
  - Push i pull opcije dohvaćanja poruka



## Identity based encryption (IBE)



# Business Email Compromise (BEC)

## Impersonation Analysis

- Identify normal Display Name / Header Address matches.
- Detect inbound email spoofing and warn recipient
- Prevent Whaling attacks against C-Levels
- Automatic detection of normal address format or manual upload

The diagram shows a flow of information related to email impersonation. At the top, a hat icon represents an impersonator, a mail box icon represents the source, and a person icon represents the recipient. An email header is shown: **Mail From:** [Ken.Xie@fortinet.com](mailto:Ken.Xie@fortinet.com) and **To:** [CFO@fortinet.com](mailto:CFO@fortinet.com). A red arrow points from the source to the recipient with the warning: **Warning: Suspected Impersonation**, accompanied by a red envelope icon.

Below the diagram are three screenshots from a security management console:

- Impersonation Entry:** Shows configuration for an impersonation profile named "IM\_test" with domain "system". The entry table lists display name patterns and email addresses.
- AntiSpam Profile:** Shows scan configurations for an "AS\_Inbound" profile. The "Impersonation analysis" rule is highlighted with a red box, showing it is configured with the "IM\_test" profile.
- Top Recipients:** A bar chart showing the top recipients of spam. The x-axis is message count (0 to 3500) and the y-axis lists recipients.

Display Name Pattern	Pattern Type	Email Address
Ken Xie	Wildcard	kxie@fortinet.com
Ken*Xie	Wildcard	*@fortinet.com

Recipient	Message Count
Spam Removal <removespam@fortinet.c...>	3008
Yan Lin <yanlin@fortinet.com>	1200
Zhaoqing Qiang <zqqliang@fortinet.com>	698
Ben Zhou <benzhou@fortinet.com>	698
FortiGuard Web Filtering Service <fgweb...>	420
Adam Shewchuk <ashewchuk@fortinet.c...>	402
jordanleee@fortinet.com	396
Lei Wang <leiwang@fortinet.com>	353
Binh Tran <btran@fortinet.com>	326
Wilson Zhang <wzhang@fortinet.com>	314

## Security Fabric

### Integration with the Fortinet Security Fabric

The future of email security is platform- or fabric-enabled to counter the growing sophistication of threats and multi-vector campaigns. As part of the Fortinet Security Fabric, Indicators of Compromise and other telemetry can be shared for enhanced security across your entire security infrastructure.

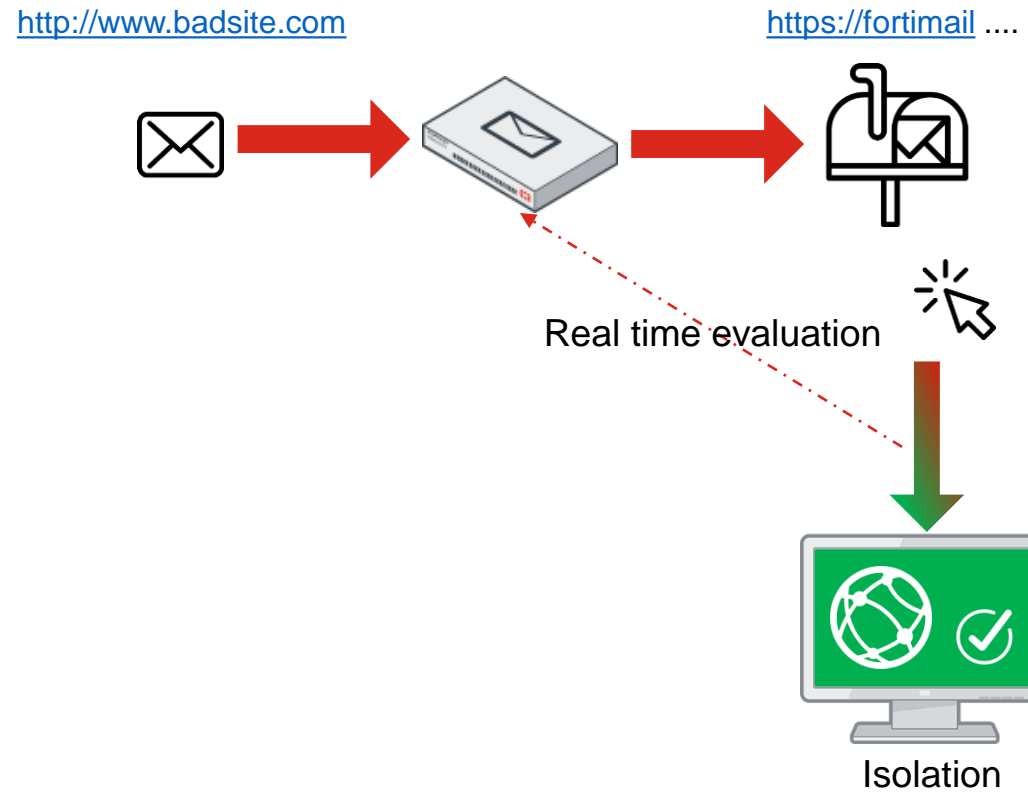
IT and security teams are able to more completely connect the dots to identify multi-vector campaigns by sophisticated actors. And intensive and repetitive workflows including response can be automated to reduce the burden on security operations teams.





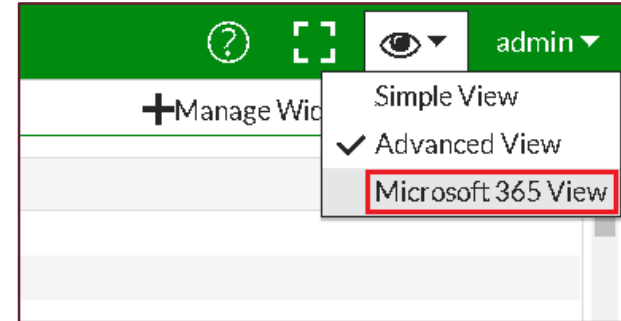
## ATP: Fortisolator integration

- Fortisolator
  - Clientless remote browsing
  - Hide user IP address from malicious servers
- Can be combined with Click Protection
- Rewriting URL from email body for safer browsing and anonymity



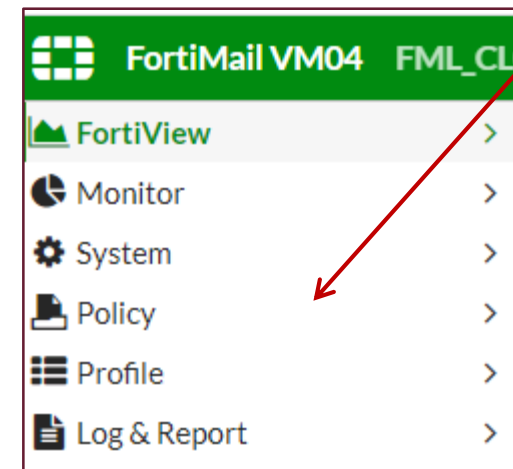
## Microsoft 365 API integracija

- **API based**
  - Out-of-band security enforcement for M365
  - Utilise M365 APIs to implement post delivery search clawback
  - Requires separate license
  - Introduces dedicated menu view
- **Real-Time Scanning**
  - Messages scanned on arrival in the user mailbox
- **On Demand Scanning / Post Delivery Clawback**
  - Messages scanned after delivery
  - Scans can be scheduled
  - Allows for manual application of actions



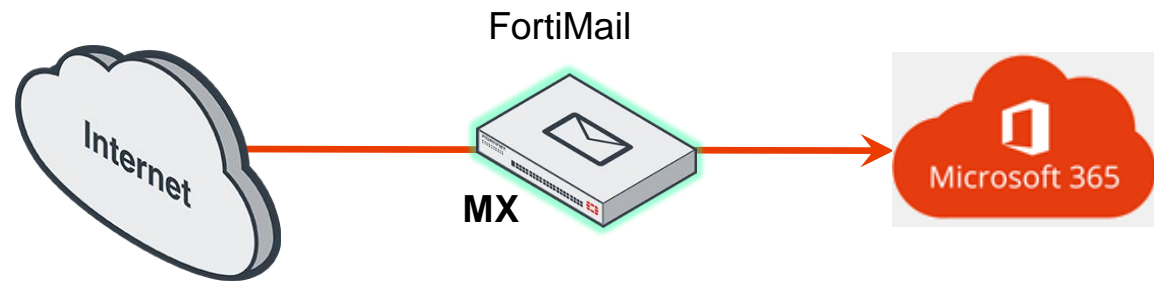
New GUI "View" for Microsoft 365 features.

Delivers simplified view of features

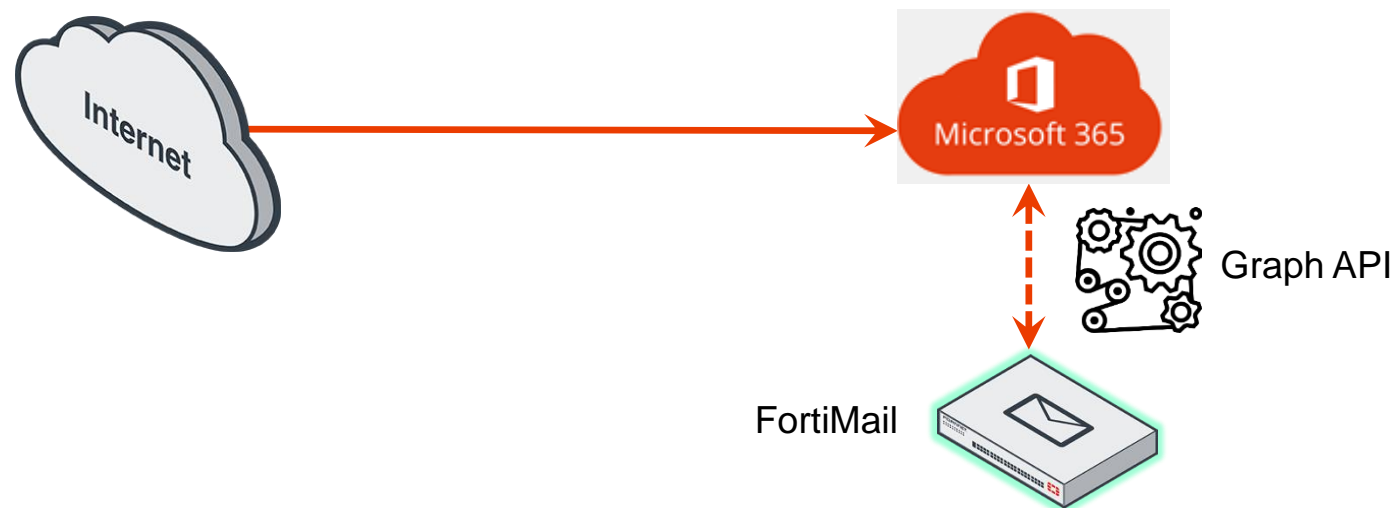




## FortiMail with Microsoft 365 architectures



Inline Mode

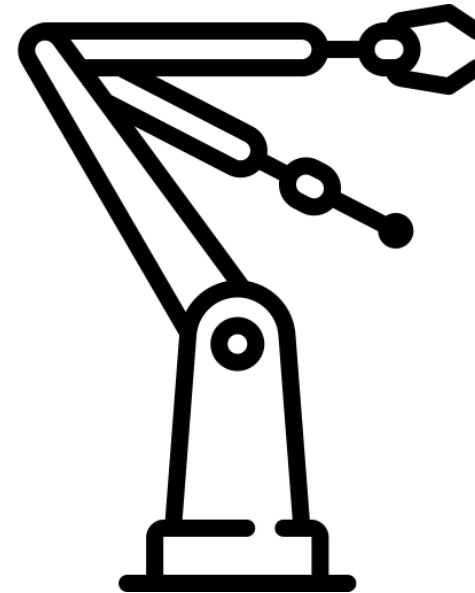


Off Path Mode

## Microsoft 365

### Direct API integration

- **Integrated security can be better**
  - More than 50% of O365 customer use third party SEG (Gartner)
- **FortiMail for MS 365 offers**
  - Better security and visibility
  - Remediation
- **Starting FML 400F/VM02**



# 24x7 + Enterprise ATP Bundle



SECURED BY  
**FORTIGUARD®**

## 24x7 + Base Bundle



### Antispam Service

- Sender IP ratings
- Embedded URL ratings
- Content-based hashes for spam and phishing campaigns
- Separate "newsletter" identifiers

À LA CARTE



### Antivirus Service

- One-to-many signatures
- Heuristic rules
- Emulation
- Decrypting/Unpacking
- Patented content pattern recognition language (CPRL)

À LA CARTE



### Outbreak Prevention

- Pre-signature intelligence
- Covers emerging spam and malware campaigns
- Leverages new sandbox and other intelligence

À LA CARTE



### FortiSandbox Cloud

- FortiSandbox hosted by Fortinet
- Includes pre-filtering, emulation and full instrumented analysis
- Subscription-based
- No separate sandbox required

À LA CARTE



### Content Disarm and Reconstruction

- Removes high risk active content
- Supports Microsoft Office and Adobe
- Can be applied by user, group or policy
- Original documents can be retained and restored



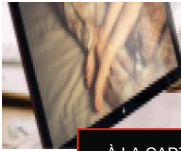
### Click Protect

- Dynamic reputation query
- Determines rating at the time of user click
- Identifies recently compromised sites changed shortly after campaigns are launched



### Impersonation Analysis

- Identifies spoofed email
- Dynamically builds protections for common email addresses
- Complements sender authentication



À LA CARTE

### Adult Image Analysis



À LA CARTE

### Direct API integration



À LA CARTE

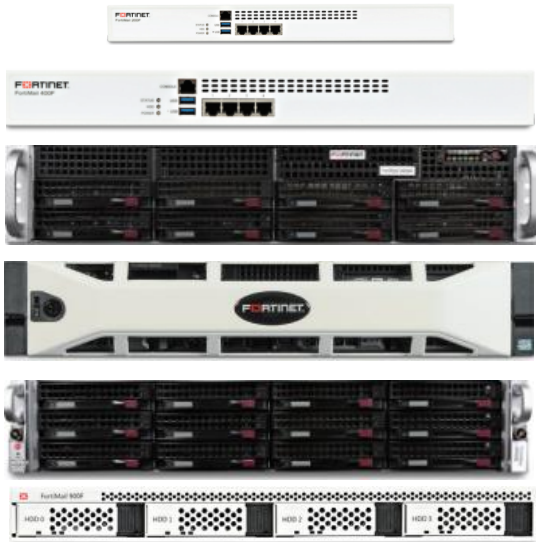
### Advanced Features



À LA CARTE

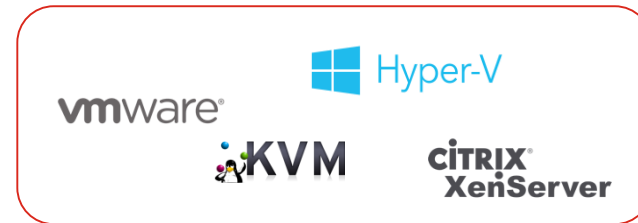
### Email Continuity

## Skalabilni form faktor za organizacije svih veličina



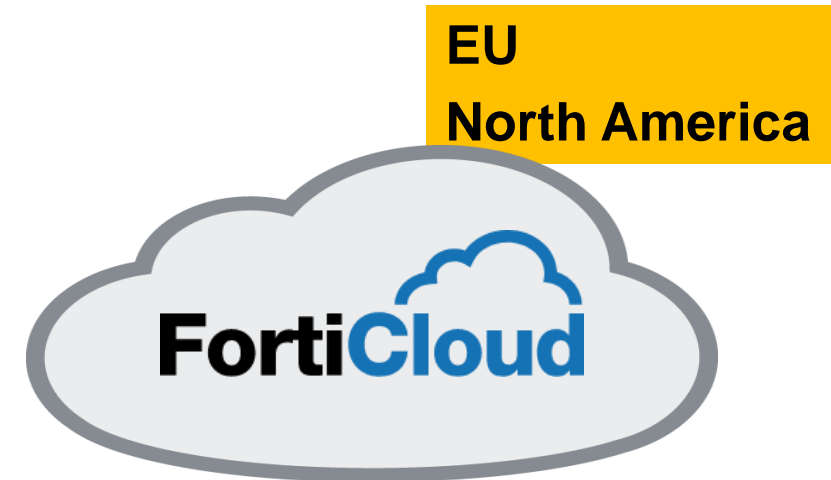
### Hardware Appliances

- 6 models
- Support for 10GE



### Virtual Appliances

- 6 VM models
- CPU- and Domain- based
- Perpetual licensing



### SaaS

- Gateway or Server Mode
- Standard or Premium
- Per User Per Year

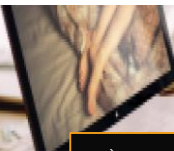
## FortiMail Cloud / SaaS : per mailbox



	Gateway	Gateway Premium	Gateway Premium O365	MSSP	MSSP monthly
AntiSpam / AntiVirus	✓	✓	✓	✓	✓
Cloud Sandboxing		✓	✓	✓	✓
Microsoft 365			✓		
Domains*	10	10	10	2000	2000
Billing	Prepaid	Prepaid	Prepaid	Prepaid	Consumption
Yearly Base Fee					✓
Mailbox Counting	Defined when service is purchased				Variable



À LA CARTE

**Email  
Continuity**


À LA CARTE

**Adult Image  
Analysis**

\* «Domains» refers to the number of Protected Domains and sub-Domains that can be created  
Note that Associated domains can be used for higher need of domains.

Fortinet FortiMail								
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	43	1	0	0	0	1	0	15
Phishing	43	5	3	9	0	0	0	0
Malware	65	0	5	0	0	0	0	0
Business Email Compromise	20	0	0	0	0	0	0	0
<b>TOTAL</b>	<b>171</b>	<b>6</b>	<b>8</b>	<b>9</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>15</b>



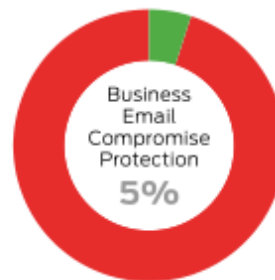
Microsoft Office 365 Advanced Threat Protection								
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	11	0	0	0	30	19	0	0
Phishing	10	0	3	1	0	1	34	11
Malware	47	1	7	0	1	14	0	0
Business Email Compromise	0	0	0	0	20	0	0	0
<b>TOTAL</b>	<b>68</b>	<b>1</b>	<b>10</b>	<b>1</b>	<b>51</b>	<b>34</b>	<b>34</b>	<b>11</b>



Fortinet FortiMail								
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	43	1	0	0	0	1	0	15
Phishing	43	5	3	9	0	0	0	0
Malware	65	0	5	0	0	0	0	0
Business Email Compromise	20	0	0	0	0	0	0	0
<b>TOTAL</b>	<b>171</b>	<b>6</b>	<b>8</b>	<b>9</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>15</b>



Google G Suite Enterprise								
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	10	0	0	0	40	10	0	0
Phishing	9	0	0	28	0	0	0	23
Malware	0	45	0	0	2	13	0	10
Business Email Compromise	1	0	0	0	0	19	0	0
<b>TOTAL</b>	<b>20</b>	<b>45</b>	<b>0</b>	<b>28</b>	<b>42</b>	<b>42</b>	<b>0</b>	<b>33</b>





**99.9%**

Detection of malicious emails across malware types and across malware families



**94%**

Overall Detection Rate



**99.78%**

Spam Catch Rate



**100%+**

Wildlist Detection Rate





# Case Study



Tommy je prema objavljenim podacima Agencije za zaštitu tržišnog natjecanja u 2020. godini i službeno **postao lider u maloprodaji Dubrovačko-neretvanske županije.**

To je vrlo značajno postignuće za našu tvrtku, jer dodatno potvrđuje da je Tommy **vodeći trgovački lanac u cijeloj Dalmaciji po svim kriterijima**, s obzirom da smo i u ostalim dalmatinskim županijama (Splitsko-dalmatinskoj, Šibensko-kninskoj i Zadarskoj) zadržali vodeće pozicije koje smo prethodno, kroz godine uspješnoga razvoja dostizali.

Također, naša tržišna pozicija jača i u drugim županijama, jednako kao i tržišni udio na nacionalnoj razini. Rezultat je to povjerenja koje su nam dali naši kupci, **prepoznajući cjelovitost i kvalitetu naše ponude**, dostupnost naših prodajnih mjesta te uslužnost i profesionalnost našega osoblja.

Liderska pozicija koju smo dostigli jasnim planom razvoja baziranom na **kontinuiranim ulaganjima u rast i razvoj poslovanja**, obvezuje nas da i dalje primjenjujemo poslovnu strategiju u kojoj su kupci njihove potrebe uvijek u prvom planu.

Veliki doprinos unapređenju pozicije Tommy-ja daju i **stalne inovacije, te uvođenje dodatnih prodajnih kanala i usluga** koje smo implementirali u prethodnom razdoblju; **online prodaja putem web shopa, usluga preuzimanja paketa na prodajnim mjestima, mogućnost plaćanja računa na Tommy blagajnama i e-punionice za vozila.**

Svakodnevno odgovaramo tržišnim izazovima, a naša je ambicija da putem realizacije budućeg razvoja dodatno ojačamo svoje pozicije, ne samo kao prepoznatljiv i relevantan trgovački lanac, već i kao vrlo poželjan poslodavac te društveno odgovorna kompanija.

# TOMMY

ZNA ŠTO VOLIŠ.



- **6. trgovački lanac u RH** s kontinuiranim rastom tržišnog udjela.
- **19. tvrtka** po ukupnom prihodu u RH.
- U 2019. godini **ostvareno 3 milijarde i 100 milijuna kuna prihoda** uz rast od 10 % u odnosu na prethodnu godinu.



- **217** prodajnih mjesta u RH, rasprostranjenih u 8 hrvatskih županija i gradu Zagrebu.
- **4 prodajna formata**  
HIPERMARKET  
MAXIMARKET  
SUPERMARKET  
MARKET
- **više od 120.000 m<sup>2</sup>** ukupnog korisnog poslovnog prostora.



- Primjena visokih ekoloških standarda kao potpora održivom razvoju i očuvanju prirode i okoliša.



- **4100 zaposlenika**



- Informacije o sustavu:
  - Hibridna instalacija - lokalni i cloud mail serveri
  - 4500 korisničkih računa
- Problemi prije implementacije:
  - SPAM
  - Blacklistanje vlastitih javnih IP adresa
  - Nedovoljne kontrole dolaznih i odlaznih mailova
  - Nedostatak izvještaja



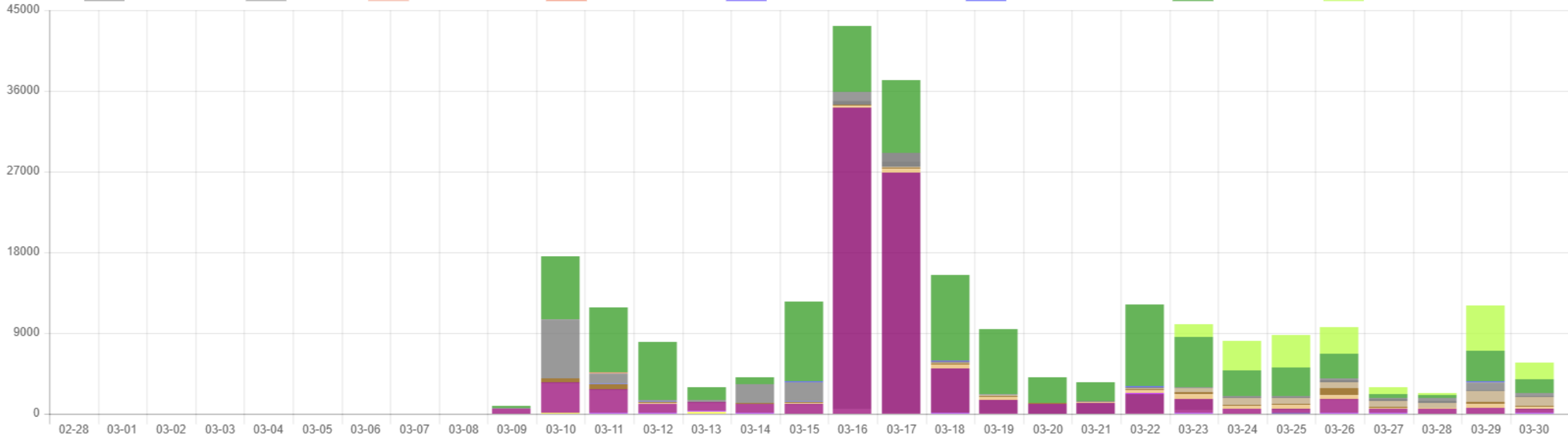
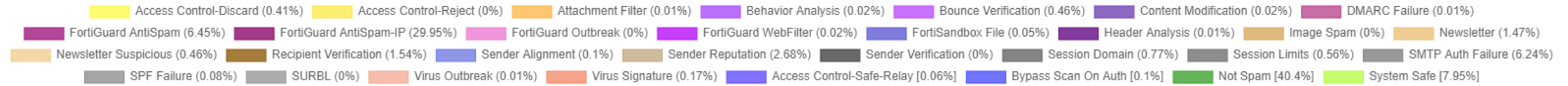
Komentar naručitelja:

*„Radi dobro, dodatna konfiguracija od ranije definiranih pravila je minimalna, odbaci veliku većinu spama, minimalne korekcije na dnevnoj bazi su potrebne za rad sustava.*

*Također nismo imali nijedan blacklist adresa od uvođenja FML.”*

## Statistika nakon implementacije FortiMail-a

Count, By Day



## FortiMail 7.0.0: Feature overview

### PRODUCTIVITY

- **FortiMail Cloud: Email continuity**

### SECURITY

- TLS profile
  - DANE
  - TLS version
- Session
  - Pipelining check
- AS
  - DKIM enforcement
  - SPF/DKIM safelist
  - Cousin domain detection
- AV
  - FSA remove URL
- SRS
- Auth Reputation
- CA repository

### OPERATION

- Dashboard: new widgets
- FortiView: outbreak stats
- Template: MESSAGE\_ID variable
- Search
  - System Quarantine enhanced
  - Log advanced and new Task search
- AS multi-action
- CDR workflow
- Document block/safe list entries
- Archive : new criteria for deferred emails
- Domain : comment field
- System Quarantine for Domain admin
- Delegate Domain admin creation

## FortiMail 7.0.0: Feature overview

### USER EXPERIENCE

- UI rework
  - FGD tabs
  - Security/Others
- Offensive terms
- Resource profile update
- New admin profile

### LICENSING

- MSSP renamed
- MSSP new maximums

### DEPLOYMENT

- Config-Sync selective attr
- New Receive Action in ACL
- FSA datacenter



## FortiMail - Business Email Continuity (BEC)

- Mitigate the impacts of backend downtime
  - Keeping end users productive during business outages
  - Providing access to their emails from the Gateway
- Reduce user recovery time to near zero
  - They can access queued email directly on FortiMail
- Adds to MS 365 security
  - Microsoft suffered several down times in the past

Certificate Bundle (version 1.00022)	Last updated (2021-04-07 17:37:21)
Microsoft 365 Protection	✓ Licensed (Expiry date 2021-12-10)
Email Continuity	✓ Licensed (Expiry date 2022-05-05)
FortiSandbox Cloud	✓ Licensed (Expiry date 2021-12-10)
Advanced Management	✓ Licensed (Expiry date 2021-12-11)



## FortiMail - Business Email Continuity (BEC)

- Cloud
  - Should be equal to the number of mailboxes
  - FC-10FMLC0-309-02-DD
- HW/VM
  - From VM02 and 400F
  - Single SKU
  - FC-10-{FE4HF/.../M3K2E/VM02/.../VM32}-309-02-DD
- Not yet available in VM S-Servies

FML\_CLOUD\_GW\_DEMO

Domain name: fml365.work

Relay type: Host

Other

Webmail theme: Use system settings

Webmail language: --Default--

Maximum message size (KB): 204800

SMTP greeting (EHLO/HELO) name (as client): Use system host name

IP pool: --None-- Direction: Delivering

Remove received header of outgoing email  
 Use global bayesian database  
 Bypass bounce verification  
 Email continuity



Domain

Dashboard FortiView Monitor System Network Administrator Configuration Mail Setting Customization High Availability Certificate FortiSandbox FortiGuard

License AntiVirus AntiSpam **Licensed Feature**

**Email Continuity**

Enable

Retention period: 30

**Advanced Management**

Enable centralized monitor  
 Enable mailbox accounting service  
 Enable domain group support  
 Enable history log access for domain level administrator  
 Enable MTA advanced control



Enable

Inbound Recipient Policy

Authentication and Access

Authentication type: LDAP

Authentication profile: fml365\_LDAP

Use for SMTP authentication

Webmail access

Dashboard FortiView Monitor Log Quarantine Mail Queue **Continuity**

**Continuity**



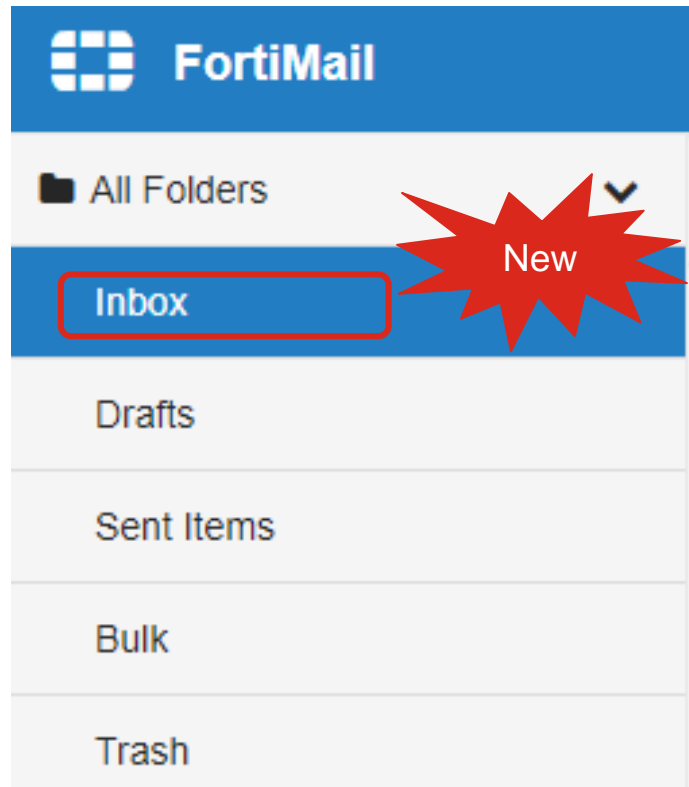
Queue

Records per page: 50

Folder	Message Count
20210505	1

Monitoring

## Webmail access



## FortiMail – Secure Email Gateway

- Sigurnosne rizike koje dolaze putem maila treba ozbiljno shvatiti, kao i pitanje cloud email zaštite
- Jedan od najbolje ocijenjenih sustava za mail zaštitu po nezavisnim testovima
- CTAP - uključuje i Email Risk Assessment
  
- Način rada: Gateway, M365 API, Transparent, Server
- Izvedbe: HW, VM, cloud, SaaS
- URI i document SandBoxing, IBE, CDR, Click protection



# Fortinet i Integra Group

Integra Group – Engage Expert partner!

# ENGAGE

**FORTINET** EXPERT PARTNER

Integrator

Data Center  
SPECIALIZATION



Secure  
SD-WAN  
SPECIALIZATION



# Q & A

Zagreb / Osijek / Rijeka / Split  
[www.integrargroup.hr](http://www.integrargroup.hr)

[prodaja@integrargroup.hr](mailto:prodaja@integrargroup.hr)  
[ivan.galinac@integrargroup.hr](mailto:ivan.galinac@integrargroup.hr)  
[nikolina.mihic@integrargroup.hr](mailto:nikolina.mihic@integrargroup.hr)